New York State Comptroller
THOMAS P. DiNAPOLI

Jericho Union Free School District

Acceptable Use Policy

2022M-194 | July 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Jericho Union Free School District

Audit Objective

Determine whether Jericho Union Free School District (District) officials helped safeguard personal, private and sensitive information (PPSI) by developing controls and communicating an acceptable use policy (AUP) to business office staff.

Key Findings

District officials did not help safeguard PPSI by developing and communicating a comprehensive AUP to business office staff. As a result, PPSI related to District employees and finances could be exposed because some websites may be malicious or contain code to compromise a user's computer or prompt the user to perform activities that may result in malware infection or PPSI exposure. In addition to sensitive information technology (IT) weaknesses that were communicated confidentially to officials, we found:

- All nine business office employees, including the Assistant Superintendent for Business Affairs (ASB), were not aware that they were expected to follow the Computer Network and Internet Student Acceptable Use policy or what the District considers to be appropriate and inappropriate Internet use.
- District officials did not periodically review web histories to determine whether any employee's web browsing was inappropriate.

Key Recommendations

- Ensure the AUP is updated, or administrative regulations are developed, to provide guidance for business office staff that defines acceptable Internet use and browsing.
- Ensure business office staff who utilize computers are adequately informed of the regulations.

District officials disagreed with certain aspects of our findings and recommendations. Appendix B includes our comments on issues raised in the District's response letter.

Background

The District is located in the Towns of Oyster Bay and North Hempstead in Nassau County and is governed by an elected five-member Board of Education (Board) responsible for the general management and control of financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Director of Educational Technology (IT Director), along with IT staff, is responsible for managing the District's IT operations.

Quick Facts

District Business Office	
Network User Accounts	9
Employees	9
Computers	12

Audit Period

July 1, 2020 – June 2, 2022

Acceptable Use Policy

Why Should Officials Develop and Communicate an Acceptable Use Policy?

Inappropriate Internet browsing and use can lead to inadvertent information being disclosed, including PPSI, or introduce viruses, ransomware and other types of malicious software into a school district's computing environment. As such, school district officials should address these risks by adopting an employee AUP that defines, among other things, what constitutes appropriate and inappropriate use of IT resources, including web browsing and Internet use, management's expectations concerning personal use and consequences for violating the AUP.

Inappropriate browsing or Internet use can include, but is not limited to:

- Viewing or sharing inappropriate or obscene material;
- Conducting activities for personal gain, such as private business or day trading; and
- Hacking or downloading unauthorized software.

Officials should develop procedures for monitoring compliance with the AUP. Procedures should include routinely monitoring Internet usage and requiring web filtering software to block access to unacceptable websites and limit access to sites that do not comply with a school district's AUP. IT officials should communicate the AUP to all employees and other individuals (e.g., consultants, vendors) who utilize the school district's computers and the Internet to perform their job duties.

Officials Did Not Develop and Communicate a Comprehensive Acceptable Use Policy

In January 1998, the Board adopted the Staff Use of Computerized Information Resources policy to address the acceptable use of computers, Internet and email. Although this policy established parameters for acceptable computer and email use and consequences for violating them, it did not describe what constitutes appropriate and inappropriate Internet browsing or use. The IT Director said that, in addition to the 1998 policy, employees were provided and expected to follow the District's Computer Network and Internet Student Acceptable Use policy that was adopted by the Board in November 2020.

We interviewed all nine business office employees, including the ASB, and found that no person was aware that they were expected to follow the Computer Network and Internet Student Acceptable Use policy or what the District considers to be appropriate and inappropriate Internet use. Responses from these employees ranged from being unaware of AUP-related policies to being verbally told that personal Internet browsing was acceptable during lunch and break times.

Additionally, District officials did not periodically review web histories to determine whether any employee's web browsing was inappropriate. The IT Director told us that in addition to utilizing web filtering, the District contracts with a third-party that monitors web traffic throughout the District and alerts IT staff of unusual activity. While the web filtering and third-party monitoring can help mitigate instances of inappropriate browsing or Internet use, periodic reviews of web history would provide a more definitive review of activity to identity inappropriate use.

In June 2022, after discussions with District officials about the AUP, the IT Director implemented a pre-login screen on District computers informing employees that, "By signing into this device, using your Jericho user account, and/or connecting to Jericho's network, you agree to abide by our Acceptable Use Policy…" However, the District did not have a policy specifically named Acceptable Use Policy. Furthermore, District officials did not describe what constitutes appropriate and inappropriate Internet browsing or use. In September 2022, after our audit fieldwork was completed, the Board adopted a revised Staff Use of Computerized Information Resources policy that included guidelines for the acceptable use of social media websites. However, the revisions did not address other Internet use, such as what constitutes inappropriate Internet browsing. Both the original and revised policies included language directing the Superintendent or his/her designee to develop administrative regulations to "implement the terms of the policy, addressing general parameters of acceptable staff conduct as well as prohibited activities." The IT Director told us that he is the Superintendent's designee responsible for developing the administrative regulations, and he acknowledged that the administrative regulations were necessary but had no explanation for why they have not been developed.

Due to the lack of guidance for employees about Internet use, we reviewed the Internet history on all 12 District computers used by business office employees to determine whether Internet activity was appropriate. We reviewed employees whose job duties required access to sensitive information related to employees (e.g., addresses, social security numbers, and direct deposit bank information) and the District's finances (e.g., bank information), including the:

- ASB,
- Treasurer/Assistant Business Manager,
- Accounts payable and payroll clerks,
- Secretary, and
- Filing clerk.

We also analyzed over 8,700 web addresses visited by business office employees and found no instances of inappropriate activity or indications that malware or unwanted programs may have been installed from the web histories we reviewed.

Although our Internet history review found no instances of inappropriate Internet browsing or indication that malware or unwanted programs were installed, PPSI related to District employees and finances could be exposed because the AUP did not provide clear expectations from the Board and management regarding acceptable Internet use. For example, some websites may be malicious or contain code to compromise a user's computer or prompt the user to perform activities that may result in malware infection or PPSI exposure. The AUP should dissuade actions such as visiting websites and downloading software or files from unknown or untrusted sources as they increase the likelihood of computers being exposed to malware.

What Do We Recommend?

The Board should:

1. Ensure that the AUP is updated, or the Superintendent or his/her designee develops administrative regulations, to provide guidance for business office staff that defines acceptable Internet use and browsing.

The IT Director should:

2. Ensure business office staff who utilize computers are adequately informed of the regulations.

3. Develop procedures for monitoring compliance with the AUP, such as routinely monitoring Internet usage.

Appendix A: Response From District Officials

Portions of the District's response were redacted for security concerns.

JERICHO UNION FREE SCHOOL DISTRICT
99 Cedar Swamp Road
Jericho, New York 11753-1202
516-203-3600

HENRY L. GRISHMAN
SUPERINTENDENT OF SCHOOLS

May 18, 2023

Public Response to the Comptroller's Office

Unit Name: Jericho UFSD
Audit Report Title: Jericho Union Free School District Acceptable Use Policy
Audit Report Number: 2022M-194

Thank you for sharing the public audit report you prepared. In reviewing the report, Dr. Patrick Fogarty, Jericho's Director of Technology, identified several concerns that he believes require further discussion. The most pressing concern is the repeated implication that the district does not have and has not had a staff acceptable use policy in place. While the comptroller's office's representatives may have felt the policy was inadequately designed or communicated, the audit report contains the following text: "District officials did not help safeguard PPSI by developing and communicating an AUP to business office staff." The district has had a policy in place since January of 1998 and can provide Board policy manuals from previous years to illustrate this. While previous AUPs are discussed further into the public report, a cursory review of this report is likely to produce a false impression in the reader. The language used in the beginning of the report is misleading. I will elaborate more on the Director of Technology's concerns about the report but would first like to share Jericho's Corrective Action Plan for the finding of this audit. This document is to serve as both our audit response and CAP.

See Note 1 Page 8

For the recommendation included in the audit report, the following are the corrective actions taken by the district.

Audit Recommendation: "Ensure the AUP is updated, or administrative regulations are developed, to provide guidance for business office staff that defines acceptable Internet use and browsing, and ensure that business office staff who utilize computers are adequately informed of the regulations."

The Director of Technology was responsible for all steps of this plan of action.

Implementation Plan of Action:

1. April-June 2022: Evaluated other districts' staff acceptable use policies and their methods of communicating these policies. Also consulted with our contracted partners [redacted] regarding best practices in staff acceptable use policies.
2. May-June 2022: Compiled a list of actions that would be considered outside the acceptable parameters of acceptable use by analyzing external companies' parameters of acceptable use and consulting with cybersecurity professionals including our contracted partners [redacted]

3. May 2022: Revised the staff acceptable use policy in accordance with best practices as determined by a review of other districts' policies, staff feedback, and recommendations from our cybersecurity partners.
4. May 2022: Received and responded to feedback on the revised acceptable use policy from staff members during the first and second policy readings at Board of Education meetings (the first reading was at the May 19, 2022 meeting).
5. June 2022: Created a parameters of acceptable use addendum to our Board of Education staff acceptable use policy and post it to our website. The date of confirmed posting is January 21, 2023, though I believe it was posted as early as September 2022.
6. June 15, 2022: Added a notice to all district PCs and Chromebooks at the login window containing the following message: "By signing into this device, using your Jericho user account, and/or connecting to Jericho's network, you agree to abide by our Acceptable Use Policy and the following Board of Education policies:
   #3320 Confidentiality of Computerized Information, January 1998
   #5830 Use of District Computers, May 2005
   #7314.10 Student Use of Computerized Information Resources, January 2008
   #6470 Staff Use of Computerized Information Resources, January 1998
   #7315 Computer Network and Internet Student Acceptable Use Policy, 2019
   #7316 Student Use of Personal Technology, July 2016
   #8261 Internet Safety/Internet Content Filtering, November 2020"
7. June 15, 2022: Sent an email to all staff (including the Business department) notifying them of the change to district device log in pages to increase awareness of existing Board of Education policies related to technology and device usage.
8. September 22, 2022: Updated staff acceptable use policy is adopted by the Board of Education at a public meeting.
9. Ongoing: The Assistant Superintendent of Business has verbally reiterated to business office staff the criticality of adhering to our staff acceptable use policy.
10. Ongoing: An annual notice is emailed to all staff reminding them that they are bound by specific Board of Education policies when accessing the DCS, using district-provided accounts, utilizing district-owned devices, or conducting any work related to or on behalf of the district.

See Note 2 Page 8

The district therefore believes it has complied with the recommendation provided in the auditor's report and that the Corrective Action Plan has been completed.

Audit Report Response

Despite the implication in the title of the public report, the district has had some form of staff acceptable use policy in place since its adoption on 1/22/1998 (as is referenced later in the report), when it was titled STAFF USE OF COMPUTERIZED INFORMATION RESOURCES (policy #6470). This policy included clear language like, "the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff" and "District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law." Furthermore, while the auditors were working with Jericho's technology staff, the Director of Technology updated this policy to be more specific and robust (adopted on 9/22/2022) and posted an addendum, PARAMETERS FOR STAFF ACCEPTABLE USE [redacted] on the district website. The auditors were notified of the revised AUP as

See Note 3 Page 8

well as the ways the Director of Technology was notifying staff including business office staff about the policies to which they must adhere, but that information was left out of the report.

Regarding communicating an AUP to Business Office Staff, the Director of Technology sent an email to all staff on 6/15/2022 explaining that a) a new message was being displayed on district PCs and Chromebooks that informs the user that, by using the device, a Jericho account, and/or accessing the network, that user is agreeing to abide by Jericho's Acceptable Use Policy and several relevant Board of Education policies (available on our website in the Board of Education section) and b) reminding users that this policies have always been in place in some form. Technology staff including the Director of Technology will continue notifying all district users of these policies on an annual basis. Again, the Director of Technology made the comptroller's office aware of this, but it is not reflected in the public report.

See Note 2 Page 8

The audit report also contains the following statement: "The IT Director told us that he is the Superintendent's designee responsible for developing the administrative regulations, and he acknowledged that the administrative regulations were necessary but had no explanation for why they have not been developed." The Director of Technology asserts that he did not have "no explanation" for this, a statement that mischaracterizes their discussion. Dr. Fogarty indicates that he acknowledged that the district did not have a written list of forbidden websites or browsing activities for staff but that our policy at the time noted, "Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements." The Director of Technology did not think it appropriate to develop these consequences outside the bounds of collective bargaining but did create a list of forbidden DCS actions that were posted to our district website.

See Note 4 Page 8

The report's misleading title notwithstanding, it is unfortunate that the Office of the State Comptroller is unwilling to revise [redacted] even when the presence of factual inaccuracies are agreed upon by all parties. A more transparent, honest approach would make these exercises significantly more valuable. The focus appears to be ensuring there is at least one finding rather than ensuring the accuracy of that finding and conveying that finding honestly.

See Note 5 Page 8

Henry L. Grishman, Superintendent of Schools

Appendix B: OSC Comments on the District's Response

Note 1

The report states the District adopted a Staff Use of Computerized Information Resources policy in January 1998 to address the acceptable use of computers, Internet and email. However, the policy did not meet the standard of a comprehensive AUP. We updated our report to more clearly indicate the District lacked a comprehensive AUP.

Note 2

The report was updated to include the implementation of the login screen notice.

Note 3

The AUP-related policy in place during audit fieldwork was missing specific guidance on appropriate and inappropriate Internet browsing or use and the Superintendent or his designee had not developed administrative regulations to that effect, also required by policy. In addition, as noted in the body of our report, the District directed staff to comply with its Acceptable Use Policy; however, the District did not have a policy with that title.

Note 4

The Staff Use of Computerized Information Resources policy adopted in January 1998 directs the Superintendent or his/her designee to develop administrative regulations addressing the parameters of acceptable staff conduct, as well as prohibited activities, to provide appropriate guidelines for employee use of the District's computer system. When asked about the regulations that would provide specific guidance to employees, the IT Director could not explain why these regulations were never developed.

Note 5

The findings in the report are supported by the evidence collected during audit fieldwork and are factually accurate.

Appendix C: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures, specifically those for user access controls over business office computers to safeguard PPSI, and interviewed business office officials to determine the adequacy of the policies and procedures.
- We interviewed business office employees to obtain an understanding of AUP communication.
- We examined the Internet browsing histories as of June 3, 2022 on the 12 computers used by business office employees to determine any instances of inappropriate Internet use and indications of malware or unwanted program installation. Among other tests, we reviewed URLs for instances of keywords, such as "install," "download," "malware," "virus," "pop-up," "popup," and "uninstall," that would indicate malware or unwanted programs may have been installed.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties